



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/748,176	12/27/2000	Yutaka Ichinoi	0102/0154	5030

21395 7590 10/01/2004

LOUIS WOO
LAW OFFICE OF LOUIS WOO
717 NORTH FAYETTE STREET
ALEXANDRIA, VA 22314

EXAMINER

HO, THOMAS M

ART UNIT	PAPER NUMBER
----------	--------------

2134

DATE MAILED: 10/01/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

09/748,176

Applicant(s)

ICHINOI ET AL.

Examiner

Thomas M Ho

Art Unit

2134

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 27 December 2000.
- 2a) ☐ This action is FINAL. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-25 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-25 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☒ All b) ☐ Some * c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
 - ☐ Certified copies of the priority documents have been received in Application No. _____.
 - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|---|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413) |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | Paper No(s)/Mail Date. _____ |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

1. Claims 1-25 are pending.

Claim Rejections - 35 USC § 102

2. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

3. Claims 1-15, 22-25 are rejected under 35 U.S.C. 102(b) as being anticipated by Stefik et al.

In reference to claim 1:

Stefik et al. (Column 15, line 20 – Column 16, line 35) disclose a contents-information transmission system comprising:

A contents-information handling apparatus to which one of different levels of at least one of copyright protection and information secrecy is assigned.

- An authentication apparatus (Column 7, line 56 – Column 8, line 10)
- Means for transmitting said one of the different levels from the contents-information handling apparatus to the authentication apparatus, where the different levels transmitted are part of the digital work (Column 25, lines 30-45)

- Means provided in the authentication apparatus for comparing said transmitted one of the different levels with a predetermined reference level. (Column 15, lines 29-36)
- Means for selectively permitting and inhibiting transmission of contents information from the authentication apparatus to the contents-information handling apparatus in response to a result of said comparing, where only if the security level and authentication works out is access to the digital work permitted. (Column 25, lines 30-45)

In reference to claim 2:

Stefik et al. discloses an authentication apparatus connectable with a contents-information handling apparatus to which one of different levels of at least one of copyright protection and information secrecy is assigned, the authentication apparatus comprising:

- Means for receiving said one of the different levels from the contents-information handling apparatus, where the different levels are received as rights. (Column 25, lines 30-45)
- Means for comparing said received one of the different levels with a predetermined reference level, where the different levels may be compared at the time of the transmission. (Column 15, lines 29-36)
- Means for selectively permitting and inhibiting transmission of contents information to the contents information handling apparatus in response to a result of said comparing, where it is understood that if the security level does not match, an authorization is not granted, that the natural course of action would be to deny transmission. (Column 7, lines 25-31)

Claim 3 is rejected for the same reasons as claim 7.

In reference to claim 4:

Stefik et al. (Column 15, line 20 – Column 16, line 35) discloses a contents-information transmission system comprising a contents information handling apparatus to which one of different levels of at least one of copyright protection and information secrecy is assigned, and an authentication apparatus connectable with the contents-information handling apparatus, the authentication apparatus deciding a level of the contents-information handling apparatus which relates to at least one of copyright protection and information secrecy, the authentication apparatus selectively permitting and inhibiting transmission of contents information to the contents-information handling apparatus in response to said decided level; the contents-information handling apparatus comprising:

- Means for storing data representative of said one of the different levels (Column 15, line 20 – Column 16, line 35)
- Means for transmitting the data representative of said one of the different levels to the authentication apparatus. (Column 25, lines 30-45)

In reference to claim 5:

Stefik et al. (Column 15, line 20 – Column 16, line 35) discloses a contents-information handling apparatus as recited in claim 4, wherein said data comprise copyrighted data, where the data represents a digital work.

In reference to claim 6:

Stefik et al. (Column 25, lines 30-45) discloses a method of data transmission between an authentication apparatus and a contents-information handling apparatus to which one of different levels of at least one of copyright protection and information secrecy is assigned, the method comprising the steps of:

- Transmitting said one of the different levels from the contents information handling apparatus to the authentication apparatus, where the different levels are transmitted with the digital work and usage rights.
- Comparing said transmitted one of the different levels with a predetermined reference level. (Column 15, lines 29-36) & (Column 25, lines 30-45)
- Selectively permitting and inhibiting transmission of contents information from the authentication apparatus to the contents information handling apparatus in response to a result of said comparing. (Column 25, lines 30-45)

In reference to claim 7:

Stefik et al. (Column 15, line 20 – Column 16, line 35) discloses a method as recited in claim 6, wherein said one of the different levels is represented by copyrighted data, where the security levels are represented with digital works, serving as the medium from which the copyrighted data are represented.

In reference to claim 8:

Stefik et al. discloses a method as recited in claim 6, further comprising the steps of:

- Transmitting predetermined data from the authentication apparatus to the contents-information handling apparatus, where the predetermined data are the usage rights associated with the document. (Column 9, lines 8-10)
- Transmitting said one of the different levels from the contents-information handling apparatus to the authentication apparatus in response to the predetermined data received by the contents-information handling apparatus, where the different levels are transmitted with the usage rights. (Column 25, lines 30-45)

In reference to claim 9:

Stefik et al. discloses a contents-information transmission system comprising a contents-information handling apparatus to which one of different levels of at least one of copyright protection and information secrecy is assigned, and an authentication apparatus deciding a level of the contents-information handling apparatus which relates to at least one of copyright protection and information secrecy, the authentication apparatus selectively permitting and inhibiting transmission of contents information to the contents-information handling apparatus in response to said decided level; a transmission medium comprising:

- Means for connecting the contents-information handling apparatus and the authentication apparatus with each other, where the content information handling apparatus and authentication system are intertwined. (Column 15, line 20 – Column 16, line 35)
- Means for enabling said one of the different levels to be transmitted from the contents-information handling apparatus to the authentication apparatus, where the different levels

may be transmitted in the usage rights as part of the digital work. (Column 25, lines 30-45)

- Means for enabling the contents information to be transmitted from the authentication apparatus to the contents-information handling apparatus, where the content information is transmitted to a rendering repository after authentication. (Column 7, lines 25-37)

In reference to claim 10:

Stefik et al. discloses a contents-information transmission system comprising:

A contents-information handling apparatus having a capability regarding at least one of copyright protection and information secrecy;

- An authentication apparatus. (Column 7, line 56 – Column 8, line 10)
- Means for transmitting data representative of said capability from the contents-information handling apparatus to the authentication apparatus, the data containing first contents information which is copyrighted, where the data are digital works and contain usage rights for copyright protection. (Column 11, lines 34-44)
- Means provided in the authentication apparatus for judging the data transmitted from the contents-information handling apparatus. (Column 7, lines 25-37)
- Means for selectively permitting and inhibiting transmission of second contents information from the authentication apparatus to the contents-information handling apparatus in response to a result of said judging (Column 7, lines 25-37)

In reference to claim 11:

Stefik et al. (Column 7, lines 25-37) discloses an authentication apparatus connectable with a contents-information handling apparatus having a capability regarding at least one of copyright protection and information secrecy, the authentication apparatus comprising:

- Means for receiving data representative of said capability from the contents-information handling apparatus, the data containing first contents information which is copyrighted, where the means to receive the data are demonstrated in the second repository being able to receive the data transmitted.
- Means for judging the received data, where the data is judged prior to its transmission to determine if all access conditions have been met.
- Means for selectively permitting and inhibiting transmission of second contents information to the contents-information handling apparatus in response to a result of said judging, where the transmission may be terminated or "inhibited" if authorization doesn't pass.

In reference to claim 12:

Stefik et al. (Column 7, lines 25-37) discloses a contents-information transmission system comprising a contents-information handling apparatus having a capability regarding at least one of copyright protection and information secrecy, and an authentication apparatus connectable with the contents-information handling apparatus, the authentication apparatus deciding whether or not the contents-information handling apparatus has a capability regarding at least one of copyright protection and information secrecy, the authentication apparatus selectively permitting

and inhibiting transmission of first contents information to the contents-information handling apparatus in response to a result of said deciding; the contents information handling apparatus in response to a result of said deciding, where the contents-information handling apparatus is the system of Stefik et al., and the authentication apparatus is the authentication process of repository 1.

the contents information handling apparatus comprising:

- Means for storing data representative of said capability of the contents-information handling apparatus, the data containing second contents information which is copyrighted, where the data is stored are digital works.
- Means for transmitting the data to the authentication apparatus, where the digital works are transmitted if authorization passes.

Claim 13 is rejected for the same reasons as claim 12.

In reference to claim 14:

Stefik et al. (Column 13, lines 59-67) discloses a method as recited in claim 13, further comprising the steps of :

- Transmitting predetermined data from the authentication apparatus to the contents-information handling apparatus, where the predetermined data transmitted is the Identification certificates issued by the authorization server.
- Transmitting the data representative of the capability from the contents-information handling apparatus to the authentication apparatus in response to the predetermined data,

where the repository requesting content can now make an access request for a digital work. (Column 7, lines 15-37)

In reference to claim 15:

Stefik et al. discloses a contents-information transmission system comprising a contents-information handling apparatus having a capability regarding at least one of a copyright protection and information secrecy, and an authentication apparatus deciding whether or not the contents-information handling apparatus has a capability regarding at least one of copyright protection and information secrecy, the authentication apparatus selectively permitting and inhibiting transmission of first contents information to the contents-information handling apparatus in response to a result of said deciding: a transmission medium comprising:

- Means for connecting the contents-information handling apparatus and the authentication apparatus with each other, where they are connected through a transmission process.
(Column 7, lines 15-37)
- Means for enabling data representative of the capability of the contents-information handling apparatus to be transmitted to the authentication apparatus, the data containing second contents information which is copyrighted, where the data that is transmitted is the digital work from repository 1 to repository 2, and the received to the “authentication apparatus” of repository 2.
- Means for enabling the first contents information to be transmitted from the authentication apparatus to the contents information handling apparatus, where the first contents information is the initial access request. (Column 7, lines 15-27)

Claim 22 is rejected for the same reasons as claim 6.

Claim 23 is substantially similar to the method of claim 6 and is rejected for the same reasons.

Claim 24 is rejected for the same reasons as claim 11.

Claim 25 is rejected for the same reasons as claim 15.

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

5. Claims 16-21 are rejected under 35 U.S.C. 103(a) as being unpatentable over Stefik et al.

In reference to claim 16:

Stefik et al. (Column 7, lines 15-37) discloses a reliability deciding apparatus for deciding a reliability of an object apparatus to which one of different reliabilities regarding information secrecy is assigned, the reliability deciding apparatus comprising:

- Means for transmitting predetermined data to the object apparatus, where the predetermined data is the data necessary to formulate an access request. (Column 7, lines 15-18)

- Means for receiving response data from the object apparatus as a reply to the transmission of the predetermined data, where in response to the access request, if authorization is passed, the digital work and usage rights are sent. (Column 7, lines 15-37)
- Means for storing information representing a plurality of public keys corresponding to the different reliabilities respectively (Column 7, lines 58-65)
- Means for selecting one from among the public keys and decrypting the response data into a decryption-resultant data in accordance with the selected public key (Column 7, lines 58-65)

Stefik et al. fails to explicitly disclose the following:

- Means for deciding whether or not the predetermined data and the decryption-resultant data are equal to each other
- Means for when it is decided that the predetermined data and the decryption-resultant data are equal to each other, deciding that a reliability of the object apparatus is equal to one of the different reliabilities which corresponds to the selected public key.

Stefik et al. however, with regards to this, does disclose that validation of the transmitted digital work/certificate is necessary. (Column 13, lines 25-30)

The Examiner takes official notice that it was well known to those of ordinary skill in the art at the time of invention to validate a digital signature or certificate by comparing the encrypted

form or the decrypted form of the data to see if they are equal. This is merely comparing two pieces of information to see if they are equal placed in the context of digital certificates and signatures.

It would have been obvious to one of ordinary skill in the art at the time of invention to decide whether or not the predetermined data and the decryption-resultant data are equal to each other in order to validate both the software, and the authenticity of the digital signatures.

Claims 17, 18, 19 is rejected for the same reasons as claim 16.

In reference to claim 20:

Stefik et al. discloses a reliability deciding apparatus for deciding a reliability of an object apparatus to which one of different reliabilities regarding information secrecy is assigned, the reliability deciding apparatus comprising:

- Means for transmitting predetermined data to the object apparatus, where the predetermined data is the access request. (Column 7, lines 15-20)
- Means for receiving response data from the object apparatus as a reply to the transmission of the predetermined data, the response data containing a data piece peculiar to the object apparatus, where the response data is the authorized and digitally signed digital work/certificate.

- Means for decrypting the response data into decryption-resultant data, where the content is encrypted by being digitally signed, and must be inherently decrypted to be made accessible.
- Means for extracting the peculiar data piece from the decryption resultant data, where extracting the data piece from the decryption resultant data is inherent to the function of decrypting the data.
- Means for executing predetermined calculation between the extracted peculiar data piece and the predetermined data to generate a calculation-resultant data piece, where the predetermined calculation to generate a calculation-resultant data piece is the verification process of verifying a digital certificate.
- Means for compressing the calculation-resultant data piece into a compression-resultant data piece according to a predetermined function, where the data piece is “compressed” in it’s digital signed form of the digital signature which is maintained for future transmissions when a repository desires to transfer the digital work to another repository.
(Column 7, lines 55-65)
- Means for storing a plurality of reference data pieces corresponding to the different reliabilities respectively, whereby the work is accessed on condition of a digital certificate, and a digital signature is inherent to the design of a digital certificate, and inherent to the design of a digital signature are unique public or private keys used to sign or create the unique digital signature, and where these plurality of keys are the references data pieces corresponding to the different reliabilities respectively. (Column 7, lines 55-65)

- Means for processing the reference data pieces into respective processing-resultant data pieces according to the predetermined function, where the digital works are received by the repositories and are processed or “unsigned” and the certificate opened through their respective decryption or “unsigned” keys. (Column 7, lines 55-65)

Stefik et al. fails to disclose

- Means for selecting one from among the processing-resultant data pieces and deciding whether or not the selected processing-resultant data piece and the compression-resultant data piece are equal to each other,
- Means for, when it is decided that the selected processing-resultant data piece and the compression-resultant data piece are equal to each other, deciding that a reliability of the object apparatus is equal to one of the different reliabilities which corresponds to the selected processing-resultant data piece.

Stefik et al. however, with regards to this, does disclose that validation of the transmitted digital work/certificate is necessary. (Column 13, lines 25-30)

It was well known to those of ordinary skill in the art at the time of invention to validate a digital signature or certificate by comparing the encrypted form or the decrypted form of the data to see if they are equal. This is merely comparing two pieces of information to see if they are equal placed in the context of digital certificates and signatures.

It would have been obvious to one of ordinary skill in the art at the time of invention to decide whether or not the selected processing-resultant data piece and the compression-resultant data pieces are equal to each other in order to validate both the software, and the authenticity of the digital signatures.

Claim 21 is rejected for the same reasons as claim 20.

Conclusion


6. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Thomas M Ho whose telephone number is (703)305-8029. The examiner can normally be reached on M-F from 8:30am – 5:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory A. Morse can be reached at (703)308-4789. The fax phone numbers for the organization where this application or proceeding is assigned are (703)746-7239 for regular communications and (703)746-7238 for After Final communications.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (703)306-5484.

TMH

September 29th, 2004


GREGORY MORSE
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

Application/Control Number: 09/748,176
Art Unit: 2134

Page 17